

# ON THE ADDITION OF SQUARES OF UNITS MODULO $n$

MOHSEN MOLLAHAJIAGHAEI

*Department of Mathematics, University of Western Ontario,  
London, Ontario, Canada N6A 5B7*

ABSTRACT. Let  $\mathbb{Z}_n$  be the ring of residue classes modulo  $n$ , and let  $\mathbb{Z}_n^*$  be the group of its units. 90 years ago, Brauer obtained a formula for the number of representations of  $c \in \mathbb{Z}_n$  as the sum of  $k$  units. Recently, Yang and Tang in [Q. Yang, M. Tang, On the addition of squares of units and nonunits modulo  $n$ , J. Number Theory., 155 (2015) 1–12] gave a formula for the number of solutions of the equation  $x_1^2 + x_2^2 = c$  with  $x_1, x_2 \in \mathbb{Z}_n^*$ . In this paper, we generalize this result. We find an explicit formula for the number of solutions of the equation  $x_1^2 + \cdots + x_k^2 = c$  with  $x_1, \dots, x_k \in \mathbb{Z}_n^*$ .

## 1. INTRODUCTION

Let  $\mathbb{Z}_n$  be the ring of residue classes modulo  $n$ , and let  $\mathbb{Z}_n^*$  be the group of its units. Let  $c \in \mathbb{Z}_n$ , and let  $k$  be a positive integer. Brauer in [1] gave a formula for the number of solutions of the equation  $x_1 + \cdots + x_k = c$  with  $x_1, \dots, x_k \in \mathbb{Z}_n^*$ . In [4] Sander found the number of representations of a fixed residue class mod  $n$  as the sum of two units in  $\mathbb{Z}_n$ , the sum of two non-units, and the sum of mixed pairs, respectively. In [3] the results of Sander were generalized into an arbitrary finite commutative ring, as sum of  $k$  units and sum of  $k$  non-units, with a combinatorial approach.

The problem of finding explicit formulas for the number of representations of a natural number  $n$  as the sum of  $k$  squares is one of the most interesting problems in number theory. For example, if  $k = 4$ , then Jacobi's four-square theorem states that this number is  $8 \sum_{m|c} m$  if  $c$  is odd and

---

*E-mail address:* [mmollaha@uwo.ca](mailto:mmollaha@uwo.ca).

2010 *Mathematics Subject Classification.* 11B13, 05C50.

*Key words and phrases.* Ring of residue classes; Squares of units; Adjacency matrix; Walks; Paley graph.

24 times the sum of the odd divisors of  $c$  if  $c$  is even. See [5] and the references given there for historical remarks.

Recently, Tóth [5] obtained formulas for the number of solutions of the equation

$$a_1x_1^2 + \cdots + a_kx_k^2 = c,$$

where  $c \in \mathbb{Z}_n$ , and  $x_i$  and  $a_i$  all belong to  $\mathbb{Z}_n$ .

Now, consider the equation

$$x_1^2 + \cdots + x_k^2 = c, \tag{1}$$

where  $c \in \mathbb{Z}_n$ , and  $x_i$  are all units in the ring  $\mathbb{Z}_n$ . We denote the number of solutions of this equation by  $\mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$ . In [6] Yang and Tang obtained a formula for  $\mathcal{S}_{sq}(\mathbb{Z}_n, c, 2)$ . In this paper we provide an explicit formula for  $\mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$ , for an arbitrary  $k$ . Our approach is combinatorial with the help of spectral graph theory.

## 2. PRELIMINARIES

In this section we present some graph theoretical notions and properties used in the paper. See, e.g., the book [2]. Let  $G$  be an additive group with identity 0. For  $S \subseteq G$ , the *Cayley graph*  $X = \text{Cay}(G, S)$  is the directed graph having vertex set  $V(X) = G$  and edge set  $E(X) = \{(a, b); b - a \in S\}$ . Clearly, if  $0 \notin S$ , then there is no loop in  $X$ , and if  $0 \in S$ , then there is exactly one loop at each vertex. If  $-S = \{-s; s \in S\} = S$ , then there is an edge from  $a$  to  $b$  if and only if there is an edge from  $b$  to  $a$ .

Let  $\mathbb{Z}_n^{*2} = \{x^2; x \in \mathbb{Z}_n^*\}$ . The *quadratic unitary Cayley graph* of  $\mathbb{Z}_n$ ,  $G_{\mathbb{Z}_n}^2 = \text{Cay}(\mathbb{Z}_n; \mathbb{Z}_n^{*2})$ , is defined as the directed Cayley graph on the additive group of  $\mathbb{Z}_n$  with respect to  $\mathbb{Z}_n^{*2}$ ; that is,  $G_{\mathbb{Z}_n}^2$  has vertex set  $\mathbb{Z}_n$  such that there is an edge from  $x$  to  $y$  if and only if  $y - x \in \mathbb{Z}_n^{*2}$ . Then the out-degree of each vertex is  $|\mathbb{Z}_n^{*2}|$ .

Let  $G$  be a graph, and let  $V(G) = \{v_1, \dots, v_n\}$ . The *adjacency matrix*  $A_G$  of  $G$  is defined in a natural way. Thus, the rows and the columns of  $A_G$  are labeled by  $V(G)$ . For  $i, j$ , if there is an edge from  $v_i$  to  $v_j$  then  $a_{v_i v_j} = 1$ ; otherwise  $a_{v_i v_j} = 0$ . We will write it simply  $A$  when no confusion can arise. For the graph  $G_{\mathbb{Z}_n}^2$  the matrix  $A$  is symmetric, provided that  $-1$  is a square mod  $n$ .

We write  $J_m$  for the  $m \times m$  all 1-matrix. The identity  $m \times m$  matrix will be denoted by  $I_m$ .

The complete graph on  $m$  vertices with loop at each vertex is denoted by  $K_m^l$ . Thus, the adjacency matrix of  $K_m^l$  is  $J_m$ .

A *walk* in a graph  $G$  is a sequence  $v_0, e_1, v_1, e_2, \dots, e_n, v_n$  so that  $v_i \in V(G)$  for every  $0 \leq i \leq n$ , and  $e_i$  is an edge from  $v_{i-1}$  to  $v_i$ , for every  $1 \leq i \leq n$ . We denote by  $w_k(G, i, j)$  the number of walks of length  $k$  from  $i$  to  $j$  in the graph  $G$ .

One application of the adjacency matrix is to calculate the number of walks between two vertices.

**Lemma 2.1.** [2, Lemma 8.1.2] *Let  $G$  be a directed graph, and let  $k$  be a positive integer. Then the number of walks from vertex  $i$  to vertex  $j$  of length  $k$  is the entry on row  $i$  and column  $j$  of the matrix  $A^k$ , where  $A$  is the adjacency matrix.*

The next theorem provides the connection between  $\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$  and  $w_k(G_{\mathbb{Z}_{p^\alpha}}^2, 0, c)$ .

**Theorem 2.2.** *Let  $p$  be an odd prime number and  $\alpha$  be a positive integer. Then*

$$\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k) = 2^k w_k(G_{\mathbb{Z}_{p^\alpha}}^2, 0, c).$$

*Proof.* Consider the graph  $G_{\mathbb{Z}_{p^\alpha}}^2$ . Let  $(x_1, \dots, x_k) \in (\mathbb{Z}_{p^\alpha}^*)^k$  such that  $x_1^2 + x_2^2 + \dots + x_k^2 = c$ . Then  $0, x_1^2, x_1^2 + x_2^2, \dots, x_1^2 + x_2^2 + \dots + x_k^2 = c$  is a walk of length  $k$  from 0 to  $c$ .

Now, let  $0 = a_0, a_1, \dots, a_k = c$  be a walk of length  $k$ . Then  $a_i - a_{i-1} = y_i^2$ , where  $y_i \in \mathbb{Z}_{p^\alpha}^*$  for  $i = 1, \dots, k$ . Hence  $y_1^2 + y_2^2 + \dots + y_k^2 = c$ . Then the set  $\{(\epsilon_k y_1, \dots, \epsilon_k y_k); \epsilon_i \in \{1, -1\}\}$  is a set of solutions of size  $2^k$ , which proves the theorem.  $\square$

The *tensor product*  $G_1 \otimes G_2$  of two graphs  $G_1$  and  $G_2$  is the graph with vertex set  $V(G_1 \otimes G_2) := V(G_1) \times V(G_2)$ , with edges specified by putting  $(u, v)$  adjacent to  $(u', v')$  if and only if  $u$  is adjacent to  $u'$  in  $G_1$  and  $v$  is adjacent to  $v'$  in  $G_2$ . It can be easily verified that the number of edges in  $G_1 \otimes G_2$  is equal to the product of the number of edges in the graphs  $G$  and  $H$ .

**Lemma 2.3.** *The adjacency matrix of  $G \otimes H$  is the tensor product of the adjacency matrices of  $G$  and  $H$ .*

The rest of paper is organized as follows. In section 3 we reduce the case  $\mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$  to the cases  $\mathcal{S}_{sq}(\mathbb{Z}_p, c, k)$  and  $\mathcal{S}_{sq}(\mathbb{Z}_{2^\alpha}, c, k)$ . We show that if  $p$  is an odd prime number, then  $G_{\mathbb{Z}_{p^\alpha}}^2 \cong G_{\mathbb{Z}_p}^2 \otimes K_{p^{\alpha-1}}^l$ . Section 4 is devoted to the study of  $\mathcal{S}_{sq}(\mathbb{Z}_p, c, k)$ , where  $p \equiv 1 \pmod{4}$ . In this section, we write  $A^k$

as a linear combination of matrices  $A$ ,  $J_p$  and  $I_p$ , and then we obtain a formula for  $\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$ . Similarly, we find a formula for  $\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$ , where  $p \equiv 3 \pmod{4}$ , in section 5. Last section, provides an explicit formula for  $\mathcal{S}_{sq}(\mathbb{Z}_{2^\alpha}, c, k)$  by direct counting.

### 3. GENERAL RESULTS

In this section, we reduce the case  $\mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$  to the cases  $\mathcal{S}_{sq}(\mathbb{Z}_p, c, k)$  and  $\mathcal{S}_{sq}(\mathbb{Z}_{2^\alpha}, c, k)$ .

The next lemma shows that the function  $n \rightarrow \mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$  is multiplicative.

**Lemma 3.1.** *Let  $m, n$  be coprime numbers. Then  $\mathcal{S}_{sq}(\mathbb{Z}_{mn}, c, k) = \mathcal{S}_{sq}(\mathbb{Z}_m, c, k) \cdot \mathcal{S}_{sq}(\mathbb{Z}_n, c, k)$ .*

*Proof.* The proof follows using the Chinese remainder theorem.  $\square$

**Lemma 3.2.** *Let  $p$  be an odd prime number, and let  $m$  be the ideal generated by  $p$  in the ring  $\mathbb{Z}_{p^\alpha}$ . Let  $u \in \mathbb{Z}_{p^\alpha}^{*2}$  and  $r \in m$ . Then  $u + r \in \mathbb{Z}_{p^\alpha}^{*2}$ .*

*Proof.* For this to happen, it is enough to show that  $1 + r$  belongs to  $\mathbb{Z}_{p^\alpha}^{*2}$ . We know that  $r$  is a nilpotent element of  $\mathbb{Z}_{p^\alpha}$ . Let  $\lambda$  be a sufficiently large integer. Then  $(1 + r)^{p^\lambda} = 1$ . Hence,  $(1 + r)^{p^\lambda + 1} = 1 + r$ .  $\square$

**Theorem 3.3.** *Let  $p$  be an odd prime number, and let  $\alpha$  be a positive integer. Then  $G_{\mathbb{Z}_{p^\alpha}}^2 \cong G_{\mathbb{Z}_p}^2 \otimes K_{p^{\alpha-1}}^l$ .*

*Proof.* Let  $m$  be the ideal generated by  $p$ , and  $\mathbb{Z}_{p^\alpha} = \bigcup_{i=1}^p (m + r_i)$ , where  $m + r_i$  is a coset of the maximal ideal  $m$  in  $\mathbb{Z}_{p^\alpha}$ . The ring  $\mathbb{Z}_{p^\alpha}/m$  is isomorphic to the field  $\mathbb{Z}_p$ . Then for each  $r \in \mathbb{Z}_{p^\alpha}$  there is a unique  $i$  and  $n_r \in m$  such that  $r = r_i + n_r$ . Let  $\psi : G_{\mathbb{Z}_{p^\alpha}}^2 \rightarrow G_{\mathbb{Z}_p}^2 \otimes K_{p^{\alpha-1}}^l$  be defined by  $\psi(r) := (r_i + m, n_r)$ . Obviously, this map is a bijection. Now, let  $(r, r')$  be a directed edge in  $G_{\mathbb{Z}_{p^\alpha}}^2$ . We show that  $(\psi(r), \psi(r'))$  is also a directed edge in  $G_{\mathbb{Z}_p}^2 \otimes K_{p^{\alpha-1}}^l$ . By definition,  $\psi(r) = (r_i + m, n_r)$  and  $\psi(r') = (r_j + m, n_{r'})$ . We have  $r' - r \in \mathbb{Z}_{p^\alpha}^{*2}$ . Thus,  $r_j - r_i + n_{r'} - n_r \in \mathbb{Z}_{p^\alpha}^{*2}$ . Hence by Lemma 3.2,  $r_j - r_i \in \mathbb{Z}_{p^\alpha}^{*2}$ . Then  $r_j - r_i + m \in (\mathbb{Z}_{p^\alpha}/m)^{*2}$ . Since the number of edges of  $G_{\mathbb{Z}_{p^\alpha}}^2$  and  $G_{\mathbb{Z}_p}^2 \otimes K_{p^{\alpha-1}}^l$  are the same, the proof is complete.  $\square$

By the aforementioned theorem, we see

$$\begin{aligned} A_{G_{\mathbb{Z}_{p^\alpha}}^2}^k &= A_{G_{\mathbb{Z}_p}^2}^k \otimes A_{K_{p^{\alpha-1}}^l}^k \\ &= A_{G_{\mathbb{Z}_p}^2}^k \otimes J_{p^{\alpha-1}}^k. \end{aligned}$$

4.  $\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$  WHERE  $p \equiv 1 \pmod{4}$ 

In this section, we find  $\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$ , where  $p$  is a prime number with  $p \equiv 1 \pmod{4}$ .

An *strongly regular graph* with parameters  $(n, k, \lambda, \mu)$  is a simple graph with  $n$  vertices that is regular of valency  $k$  and has the following properties:

- For any two adjacent vertices  $x, y$ , there are exactly  $\lambda$  vertices adjacent to both  $x$  and  $y$ .
- For any two non-adjacent vertices  $x, y$ , there are exactly  $\mu$  vertices adjacent to both  $x$  and  $y$ .

Let  $p$  be a fixed prime number with  $p \equiv 1 \pmod{4}$ . The Paley graph  $P_p$  is defined by taking the field  $\mathbb{Z}_p$  as vertex set, with two vertices  $x$  and  $y$  joined by an edge if and only if  $x - y$  is a nonzero square in  $\mathbb{Z}_p$ .

As is well known (see e.g., [2, Page 221]), the Paley graph is strongly regular with parameters  $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$ . The fact that Paley graph is strongly regular shows that  $A^2$  can be written as a linear combination of matrices  $A$ ,  $J_p$  and  $I_p$ .

**Lemma 4.1.** [2, Page 219] *Let  $p$  be a prime number such that  $p \equiv 1 \pmod{4}$ . Then the adjacency matrix of the Paley graph  $P_p$  satisfies*

$$A_{P_p}^2 = -A_{P_p} + \left(\frac{p-1}{4}\right)J_p + \left(\frac{p-1}{4}\right)I_p. \quad (2)$$

Although the graph  $G_{\mathbb{Z}_p}^2$  is a directed graph and  $P_p$  is a simple graph, they share the same adjacency matrix. Then  $A_{G_{\mathbb{Z}_p}^2}^n$  can be written as a linear combination of  $A_{G_{\mathbb{Z}_p}^2}$ ,  $I_p$  and  $J_p$ .

Let

$$A^{n+1} = a_{n,p}A + b_{n,p}J_p + c_{n,p}I_p. \quad (3)$$

Then

$$A^{n+2} = a_{n,p}A^2 + \frac{p-1}{2}b_{n,p}J_p + c_{n,p}A.$$

Now, by equation (2), we have

$$A^{n+2} = (a_{n,p}a_{1,p} + c_{n,p})A + \left(\frac{p-1}{2}b_{n,p} + a_{n,p}b_{1,p}\right)J_p + (a_{n,p}c_{1,p})I_p.$$

Then we see that

$$\begin{cases} a_{n+1,p} = a_{n,p}a_{1,p} + c_{n,p}, & a_{1,p} = -1, a_{2,p} = \frac{p+3}{4}; \\ b_{n+1,p} = \frac{p-1}{2}b_{n,p} + a_{n,p}b_{1,p}, & b_{1,p} = \frac{p-1}{4}, b_{2,p} = \left(\frac{p-1}{4}\right)\left(\frac{p-3}{2}\right); \\ c_{n+1,p} = a_{n,p}c_{1,p}, & c_{1,p} = \frac{p-1}{4}, c_{2,p} = -\frac{p-1}{4}. \end{cases}$$

From the first and last equations, we have the following homogeneous linear recurrence relation

$$a_{n,p} = \frac{p-1}{4}a_{n-2,p} - a_{n-1,p}.$$

Since  $a_1 = -1$  and  $a_2 = \frac{p+3}{4}$ , we deduce

$$a_{n,p} = \left(\frac{\sqrt{p}-1}{2\sqrt{p}}\right)\left(\frac{-1+\sqrt{p}}{2}\right)^n + \left(\frac{\sqrt{p}+1}{2\sqrt{p}}\right)\left(\frac{-1-\sqrt{p}}{2}\right)^n.$$

Then

$$a_{n,p} = \left(\frac{1}{2^{n+1}\sqrt{p}}\right)\left((-1+\sqrt{p})^{n+1} + (-1)^n(1+\sqrt{p})^{n+1}\right). \quad (i)$$

Now, we have

$$c_{n,p} = \left(\frac{p-1}{2^{n+2}\sqrt{p}}\right)\left((-1+\sqrt{p})^n + (-1)^{n-1}(1+\sqrt{p})^n\right). \quad (ii)$$

Thus, for  $b_{n,p}$  we have the following non-homogeneous linear recurrence relation

$$b_{n,p} = \frac{p-1}{2}b_{n-1,p} + \left(\frac{p-1}{2^{n+1}\sqrt{p}}\right)\left((-1+\sqrt{p})^{n-1} + (-1)^{n-2}(1+\sqrt{p})^{n-1}\right).$$

Then

$$b_{n,p} = \beta\left(\frac{p-1}{2}\right)^n + \left(\frac{p-1}{2^{n+1}\sqrt{p}}\right)\left(\frac{\sqrt{p}+1}{\sqrt{p}-1}(-1+\sqrt{p})^{n-1} + (-1)^{n-2}\frac{\sqrt{p}-1}{\sqrt{p}+1}(1+\sqrt{p})^{n-1}\right).$$

Since  $b_1 = \frac{p-1}{4}$ , it follows that

$$b_{n,p} = \frac{(p-5)}{2(p-1)}\left(\frac{p-1}{2}\right)^n + \left(\frac{p-1}{2^{n+1}\sqrt{p}}\right)\left(\frac{\sqrt{p}+1}{\sqrt{p}-1}(-1+\sqrt{p})^{n-1} + (-1)^{n-2}\frac{\sqrt{p}-1}{\sqrt{p}+1}(1+\sqrt{p})^{n-1}\right). \quad (iii)$$

We can now find  $\mathcal{S}_{sq}(\mathbb{Z}_p, c, k)$ .

$$\mathcal{S}_{sq}(\mathbb{Z}_p, c, k) = \begin{cases} 2^k(b_{k-1,p} + c_{k-1,p}), & \text{if } c = 0; \\ 2^k(a_{k-1,p} + b_{k-1,p}), & \text{if } c = x^2, \text{ for some } x \in \mathbb{Z}_p^*; \\ 2^k b_{k-1,p}, & \text{otherwise.} \end{cases} \quad (4)$$

The last theorem of this section provides a formula for  $\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$ .

**Theorem 4.2.** *Let  $p$  be a prime number such that  $p \equiv 1 \pmod{4}$ . Let  $\alpha$  be a positive integer. Then*

$$\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k) = \begin{cases} p^{(\alpha-1)(k-1)}2^k(b_{k-1,p} + c_{k-1,p}), & \text{if } c \equiv 0 \pmod{p}; \\ p^{(\alpha-1)(k-1)}2^k(a_{k-1,p} + b_{k-1,p}), & \text{if } c = x^2, \text{ for some } x \in \mathbb{Z}_{p^\alpha}^*; \\ p^{(\alpha-1)(k-1)}2^k b_{k-1,p}, & \text{otherwise,} \end{cases}$$

where  $a_{k-1,p}$ ,  $c_{k-1,p}$  and  $b_{k-1,p}$  are defined by equations (i), (ii) and (iii), respectively, (putting  $n = k - 1$ ).

*Proof.* By Theorem 3.3 and Lemma 2.3,  $A_{G_{\mathbb{Z}_p}^2} = A_{G_{\mathbb{Z}_p}^2} \otimes A_{K_{p^{\alpha-1}}}$ . Then

$$\begin{aligned} A_{G_{\mathbb{Z}_p}^2}^k &= A_{G_{\mathbb{Z}_p}^2}^k \otimes J_{p^{\alpha-1}}^k \\ &= A_{G_{\mathbb{Z}_p}^2}^k \otimes p^{(\alpha-1)(k-1)} J_{p^{\alpha-1}}. \end{aligned}$$

Then equation (4) and Lemma 2.1, complete the proof.  $\square$

### 5. $S_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$ WHERE $p \equiv 3 \pmod{4}$

In this section, we find  $S_{sq}(\mathbb{Z}_{p^\alpha}, c, k)$ , where  $p$  is a prime number with  $p \equiv 3 \pmod{4}$ . The main idea is similar to that used in the previous section. We try to write  $A_{G_{\mathbb{Z}_p}^2}^2$  as a linear combination of matrices  $A_{G_{\mathbb{Z}_p}^2}$ ,  $I_p$  and  $J_p$ .

The field  $\mathbb{Z}_p$ , has no square root of -1. Then for each pair of  $(x, y)$  of distinct elements of  $\mathbb{Z}_p$ , either  $x - y$  or  $y - x$ , but not both, is a square of a nonzero element. Hence in the graph  $G_{\mathbb{Z}_p}^2$ , each pair of distinct vertices is linked by an arc in one and only one direction. Therefore,  $A_{G_{\mathbb{Z}_p}^2} + A_{G_{\mathbb{Z}_p}^2}^T = J_p - I_p$ . The entry on row  $a$  and column  $b$  of the matrix  $A_{G_{\mathbb{Z}_p}^2}^2$  equals to the size of the set  $(a + \mathbb{Z}_p^{*2}) \cap (b - \mathbb{Z}_p^{*2})$ . The goal of following lemmas is to find  $|(a + \mathbb{Z}_p^{*2}) \cap (b - \mathbb{Z}_p^{*2})|$ .

**Lemma 5.1.** *Let  $a$  and  $b$  be elements of  $\mathbb{Z}_p$ . Then  $|(a + \mathbb{Z}_p^{*2}) \cap (b - \mathbb{Z}_p^{*2})| = |(a - b + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}|$ .*

*Proof.* Let  $\psi : (a + \mathbb{Z}_p^{*2}) \cap (b - \mathbb{Z}_p^{*2}) \longrightarrow (a - b + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}$  be defined by  $\psi(r) = r - b$ . Obviously,  $\psi$  is well-defined and injective. Now, let  $c \in (a - b + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}$ , so there exists  $s \in \mathbb{Z}_p^{*2}$  such that  $c = a - b + s$ . Then  $\psi(c + b) = c$ , which completes the proof.  $\square$

**Lemma 5.2.** *Let  $a$  be a non-zero element of  $\mathbb{Z}_p$ . Then  $|(a^2 + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}| = |(1 + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}|$  and  $|(-a^2 + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}| = |(-1 + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}|$ .*

*Proof.* Let  $\psi : (a^2 + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2} \longrightarrow (1 + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}$  be defined by  $\psi(r) = ra^{-2}$ . Obviously,  $\psi$  is well-defined and injective. Now, let  $c \in (1 + \mathbb{Z}_p^{*2}) \cap -\mathbb{Z}_p^{*2}$ . Thus, there exists  $s \in \mathbb{Z}_p^*$  such that  $c = 1 + s^2$ . Then  $\psi(ca^2) = c$ , which completes the proof.

The proof for the second part is similar.  $\square$

Then by Lemmas 5.1 and 5.2, one can easily see that  $A^2$  is a linear combination of matrices  $A$ ,  $J_p$  and  $I_p$ .

**Lemma 5.3.**  $|(1 + \mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})| = \frac{p+1}{4}$ .

*Proof.* We know that  $\left((1 + \mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})\right) \cup \left((1 + \mathbb{Z}_p^{*2}) \cap (\mathbb{Z}_p^{*2})\right) = 1 + \mathbb{Z}_p^{*2}$ , and  $\left((1 + \mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})\right) \cap \left((1 + \mathbb{Z}_p^{*2}) \cap (\mathbb{Z}_p^{*2})\right) = \emptyset$ . Then  $|(1 + \mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})| = \frac{p-1}{2} - |(1 + \mathbb{Z}_p^{*2}) \cap (\mathbb{Z}_p^{*2})|$ . Now,  $a \in (1 + \mathbb{Z}_p^{*2}) \cap (\mathbb{Z}_p^{*2})$  if and only there exist  $b, c \in \mathbb{Z}_p^*$  such that  $a = 1 + b^2 = c^2$ . Thus,  $(c - b)(c + b) = 1$ . Hence  $c = \frac{u+u^{-1}}{2}$  and  $b = \frac{u-u^{-1}}{2}$ , for  $u \in \mathbb{Z}_p^* - \{1, -1\}$ . Then  $(1 + \mathbb{Z}_p^{*2}) \cap (\mathbb{Z}_p^{*2}) = \{(\frac{u+u^{-1}}{2})^2; u \in \mathbb{Z}_p^* - \{1\}\}$ .

If  $(\frac{u+u^{-1}}{2})^2 = (\frac{v+v^{-1}}{2})^2$ , then we have two cases:

- (i)  $\frac{u+u^{-1}}{2} = \frac{v+v^{-1}}{2}$ . A trivial verification shows that  $u = v$  or  $u = v^{-1}$ .
- (ii)  $\frac{u+u^{-1}}{2} = -\frac{v+v^{-1}}{2}$ . Then  $u = -v$  or  $u = -v^{-1}$ .

Then  $|(1 + \mathbb{Z}_p^{*2}) \cap (\mathbb{Z}_p^{*2})| = \frac{p-1-2}{4}$ , and the lemma follows.  $\square$

The following lemma may be proved in much the same way as Lemma 5.3.

**Lemma 5.4.**  $|(-1 + \mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})| = \frac{p-3}{4}$ .

**Lemma 5.5.** Let  $p$  be a prime number with  $p \equiv 3 \pmod{4}$ . Let  $A$  be the adjacency matrix of the graph  $G_{\mathbb{Z}_p}^2$ . Then

$$A^2 = -A + \left(\frac{p+1}{4}\right)J_p - \left(\frac{p+1}{4}\right)I_p. \quad (5)$$

*Proof.* Let  $a, b \in \mathbb{Z}_p$ . By Lemma 5.1,

$$(A)_{ab} = |(a + \mathbb{Z}_p^{*2}) \cap (b - \mathbb{Z}_p^{*2})| = |(a - b + \mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})|.$$

If there is an edge from  $a$  to  $b$ , then by Lemmas 5.2 and 5.4,

$$(A)_{ab} = |(-1 + \mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})| = \frac{p-3}{4}.$$

If  $a \neq b$  and there is no edge from  $a$  to  $b$ , then by a similar argument, we have  $(A)_{ab} = \frac{p+1}{4}$ . If  $a = b$ , then by Lemma 5.1,

$$(A)_{ab} = |(a + \mathbb{Z}_p^{*2}) \cap (b - \mathbb{Z}_p^{*2})| = |(\mathbb{Z}_p^{*2}) \cap (-\mathbb{Z}_p^{*2})| = 0,$$

which establishes equation (5).  $\square$



Let

$$A^{n+1} = a_{n,p}A + b_{n,p}J_p + c_{n,p}I_p.$$

Hence

$$A^{n+1} = a_{n,p}A^2 + b_{n,p}\frac{p-1}{2}J_p + c_{n,p}A.$$

Then

$$A^{n+1} = (c_{n+1,p} - a_{n,p})A + (a_{n,p}\frac{p+1}{4} + b_{n+1,p}\frac{p-1}{2})J_p + (-a_{n,p}\frac{p+1}{4})I_p.$$

Thus, we have

$$\begin{cases} a_{n+1,p} = c_{n,p} - a_{n,p}, & a_{1,p} = -1, a_{2,p} = \frac{3-p}{4}; \\ b_{n+1,p} = \frac{p-1}{2}b_{n,p} + a_{n,p}\frac{p+1}{4}, & b_{1,p} = \frac{p+1}{4}, b_{2,p} = \frac{p+1}{4}(\frac{p-1}{2} - 1); \\ c_{n+1,p} = -a_{n,p}\frac{p+1}{4}, & c_{1,p} = -\frac{p+1}{4}, c_{2,p} = \frac{p+1}{4}. \end{cases}$$

From the first and last equations, we have the following homogeneous linear recurrence relation

$$a_{n+1,p} + a_{n,p} + \frac{p+1}{4}a_{n-1,p} = 0.$$

Since  $a_{1,p} = -1$  and  $a_{2,p} = \frac{3-p}{4}$ , we deduce

$$a_{n,p} = \left(\frac{\sqrt{p}+i}{2\sqrt{p}}\right)\left(\frac{-1+i\sqrt{p}}{2}\right)^n + \left(\frac{\sqrt{p}-i}{2\sqrt{p}}\right)\left(\frac{-1-i\sqrt{p}}{2}\right)^n, \quad (\text{i}')$$

where  $i = \sqrt{-1}$ . Then

$$c_{n,p} = -\frac{p+1}{4}\left(\left(\frac{\sqrt{p}+i}{2\sqrt{p}}\right)\left(\frac{-1+i\sqrt{p}}{2}\right)^{n-1} + \left(\frac{\sqrt{p}-i}{2\sqrt{p}}\right)\left(\frac{-1-i\sqrt{p}}{2}\right)^{n-1}\right). \quad (\text{ii}')$$

Thus, for  $b_{n,p}$  we have the following non-homogeneous linear recurrence relation

$$b_{n,p} = \frac{p-1}{2}b_{n-1,p} + \frac{p+1}{4}\left(\left(\frac{\sqrt{p}+i}{2\sqrt{p}}\right)\left(\frac{-1+i\sqrt{p}}{2}\right)^{n-1} + \left(\frac{\sqrt{p}-i}{2\sqrt{p}}\right)\left(\frac{-1-i\sqrt{p}}{2}\right)^{n-1}\right).$$

Then

$$b_{n,p} = \alpha\left(\frac{p-1}{2}\right)^n + \frac{p+1}{8\sqrt{p}}\left(\left(\frac{(\sqrt{p}+i)(i\sqrt{p}-1)}{i\sqrt{p}-p}\right)\left(\frac{-1+i\sqrt{p}}{2}\right)^{n-1} + \left(\frac{(\sqrt{p}-i)(i\sqrt{p}+1)}{i\sqrt{p}+p}\right)\left(\frac{-1-i\sqrt{p}}{2}\right)^{n-1}\right).$$

Since  $b_{1,p} = \frac{p+1}{4}$ , it follows that

$$b_{n,p} = \frac{p-1}{2p}\left(\frac{p-1}{2}\right)^n + \frac{p+1}{8\sqrt{p}}\left(\left(\frac{(\sqrt{p}+i)(i\sqrt{p}-1)}{i\sqrt{p}-p}\right)\left(\frac{-1+i\sqrt{p}}{2}\right)^{n-1} + \left(\frac{(\sqrt{p}-i)(i\sqrt{p}+1)}{i\sqrt{p}+p}\right)\left(\frac{-1-i\sqrt{p}}{2}\right)^{n-1}\right). \quad (\text{iii}')$$

Then the number of solutions of the equation (1) is

$$\mathcal{S}_{sq}(\mathbb{Z}_p, c, k) = \begin{cases} 2^k(b_{k-1,p} + c_{k-1,p}), & \text{if } c = 0; \\ 2^k(a_{k-1,p} + b_{k-1,p}), & \text{if } c = x^2, \text{ for some } x \in \mathbb{Z}_p^*; \\ 2^k b_{k-1,p}, & \text{otherwise.} \end{cases}$$

**Theorem 5.6.** *Let  $p$  be a prime number such that  $p \equiv 3 \pmod{4}$ . Let  $\alpha$  be a positive integer. Then*

$$\mathcal{S}_{sq}(\mathbb{Z}_{p^\alpha}, c, k) = \begin{cases} p^{(\alpha-1)(k-1)} 2^k(b_{k-1,p} + c_{k-1,p}), & \text{if } c \equiv 0 \pmod{p}; \\ p^{(\alpha-1)(k-1)} 2^k(a_{k-1,p} + b_{k-1,p}), & \text{if } c = x^2, \text{ for some } x \in \mathbb{Z}_{p^\alpha}^*; \\ p^{(\alpha-1)(k-1)} 2^k b_{k-1,p}, & \text{otherwise,} \end{cases}$$

where  $a_{k-1,p}$ ,  $c_{k-1,p}$  and  $b_{k-1,p}$  are defined by equations (i'), (ii') and (iii'), respectively, (putting  $n = k - 1$ ).

*Proof.* The proof is similar to that of Theorem 4.2. □

## 6. $\mathcal{S}_{sq}(\mathbb{Z}_{2^\alpha}, c, k)$

In this section we find  $\mathcal{S}_{sq}(\mathbb{Z}_{2^\alpha}, c, k)$ . For  $\alpha = 1$  and  $\alpha = 2$ , this number is easy to find.

**Lemma 6.1.** *Let  $n = 2^\alpha$  such that  $\alpha > 2$ . Then  $\mathbb{Z}_n^{*2} = \{8k + 1; k \in \{0, \dots, \frac{n}{8} - 1\}\}$ .*

*Proof.* Obviously,  $\{8k + 1; k \in \{0, \dots, \frac{n}{8} - 1\}\} \supseteq \mathbb{Z}_n^{*2}$ . It suffices to show that the set  $\mathbb{Z}_n^{*2}$  has exactly  $n/8$  elements. Define the equivalence relation between odd elements of  $\mathbb{Z}_n$  as follows. We say  $a \sim b$  if and only if  $a^2 \equiv b^2 \pmod{2^\alpha}$ . It is easy to check that each equivalence class has exactly 4 elements. Hence the number of equivalence classes is  $n/8$ , which equals to the size of  $\mathbb{Z}_n^{*2}$ . □

Now, we are able to find  $\mathcal{S}_{sq}(\mathbb{Z}_{2^\alpha}, c, k)$ .

**Theorem 6.2.** *Let  $n = 2^\alpha$ . Then*

$$\mathcal{S}_{sq}(\mathbb{Z}_{2^\alpha}, c, k) = \begin{cases} 1, & \text{if } \alpha = 1 \text{ and } c \equiv k \pmod{2}; \\ 2^k, & \text{if } \alpha = 2 \text{ and } c \equiv k \pmod{4}; \\ 2^{2k+(\alpha-3)(k-1)}, & \text{if } \alpha > 2 \text{ and } c \equiv k \pmod{8}; \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* Let  $\alpha > 2$ . Let  $A = \{(y_1, \dots, y_k); 8 \sum_{i=1}^k y_i = c - k\}$  and  $B = \{(x_1, \dots, x_k); \sum_{i=1}^k x_i^2 = c\}$ . Then by Lemma 6.1, there exists a  $4^k$  to 1 and onto map from  $B$  to  $A$ . It is easy to see that if  $c \equiv k \pmod{8}$ , then  $|A| = (2^{\alpha-3})^{k-1}$ , which establishes the formula.  $\square$

**Remark.** Let  $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ . Then by Lemma 3.1, we conclude that

$$\mathcal{S}_{sq}(\mathbb{Z}_n, c, k) = \prod_{i=1}^t \mathcal{S}_{sq}(\mathbb{Z}_{p_i^{\alpha_i}}, c, k),$$

which can be computed easily by Theorems 4.2, 5.6 and 6.2.

### Acknowledgments.

The author deeply thanks Dariush Kiani for encouragement. The author also thanks the referee for careful reading and useful comments.

### REFERENCES

- [1] A. Brauer, Lösung der Aufgabe 30, Jahresber. Dtsch. Math.-Ver. 35 (1926) 92–94.
- [2] C. Godsil, G. Royle, Algebraic Graph Theory, Springer, New York, 2001.
- [3] D. Kiani, M. Mollahajaghahi, On the addition of units and non-units in finite commutative rings, Rocky Mountain J. Math. 45 (6) (2015), 1887–1896.
- [4] J. W. Sander, On the addition of units and nonunits mod  $m$ , J. Number Theory., 129 (2009), 2260–2266.
- [5] L. Tóth, Counting solutions of quadratic congruences in several variables revisited, J. Integer Seq. 17 (2014), Article 14.11.6.
- [6] Q. Yang, M. Tang, On the addition of squares of units and nonunits modulo  $n$ , J. Number Theory., 155 (2015) 1–12.